

# Channel Islands Live Broadcast Network and Equipment Requirements

(For Technical Staff)

## Basic Requirements:

1. **Connection to the Internet – 768Kbps is the minimum bandwidth needed** (check with your tech folks if you don't know what the connection rate is or try <http://www.speedtest.net> \* to get an estimate).
2. **Videoconferencing connection** (i.e. {a} Cisco™ Telepresence, Polycom™, Tandberg™, LifeSize, or similar video conferencing device\*), **or {b} a PC or Mac computer available that has videoconferencing software installed.**
  - a. See “Preparing for a Channel Islands Live Broadcast Using Videoconferencing Equipment”:  
<http://www.nps.gov/chis/planyourvisit/upload/Preparing-for-a-CHIL-Broadcast-Using-Videoconferencing-Equipment.pdf>
  - b. See “Preparing for a Channel Islands Live Broadcast Using Videoconferencing Software”:  
<http://www.nps.gov/chis/planyourvisit/upload/Preparing-for-a-CHIL-Broadcast-Using-Videoconferencing-Software.pdf>
3. **Good quality projector, large screen monitor, or interactive whiteboard** that the students can easily see—check the lighting in the room to make sure the image is clear (you may have to turn off lights or close window blinds as necessary to minimize backlighting).
4. **Audio system** (external speakers, interactive whiteboard, etc.) that can be set loud enough for everyone to hear clearly.
5. **Microphone** that students can get to so they can interact with the ranger on the other end. An integral microphone will work but an external USB microphone works best).
6. **Webcam** (integral or USB) so the park ranger can see you too. Please be aware of your school's Media Release/Consent Form requirements. Be prepared to point the web camera away from the students so that their images are not broadcast out to the Internet.
7. **Allow SIP specific TCP / UDP ports outbound through firewall** (see Network Setup below).

## Network Setup:

- Open firewall or router ports throughout your network all the way to the classroom wall jack.

### Allow Outbound Only:

1719 UDP - RAS Messaging  
1720 TCP - Call Connect signaling  
2776 TCP - Call Setup/Capabilities Exchange  
2776 UDP - RTP Media  
2777 UDP - RTCP Media  
5060 UDP – SIP Signaling  
5060 TCP – SIP Signaling

- **Cisco™ Specific Setup:**

- 1) PIX Firewall - You can use the **fixup** command to change the default TCP port assignment for the Session Initiation Protocol (SIP). The command syntax is as follows: **[no] fixup protocol sip <udp> [port[-port]]**

To change the default port assignments from 5060 use the *port* option. Use the *-port* option to apply SIP application inspection to a range of port numbers.

To view the current timeout value for SIP connections, enter the following command: **show timeout sip**

To view the state of SIP connections, enter the following command: **show conn state sip**

To support SIP calls through the PIX Firewall, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

To view information about the SIP sessions established across the PIX Firewall, enter the following command: **show sip**

For further information about using this command to troubleshoot CTIQBE application inspection issues, refer to the show sip command in the Cisco<sup>™</sup> PIX Firewall Command Reference.

2) ASA

An addition to your firewall is to add TCP/UDP inspection.

**class class\_sip\_udp**

**inspect sip**

**class class\_sip\_tcp**

**inspect sip**

3) Change the SIP timeout to 0:00:00

eg:

timeout xlate 3:00:00

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

**timeout sip 0:00:00 sip\_media 0:00:00 sip-invite 0:03:00 sip-disconnect 0:02:00**

**timeout sip-provisional-media 0:02:00** uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

4) It has been observed the on some “older IOS” Cisco<sup>™</sup> firewalls the “inspect sip” statement has the effect of breaking sip sessions. To correct this abnormal functionality it has been necessary to disable “inspect sip” and allow inbound traffic from 207.157.245.40 on ports >=1024 destined to your software or telepresence device.

### **Troubleshooting Tips:**

1. Telnet from a host at the wall jack via port 5060 to 207.157.245.40. You should get some sort of connection vs. an outright denial (i.e., >telnet 207.157.245.40 5060).
2. Check your firewall logs for blocked traffic from "207.157.245.40"
3. Check your firewall logs for blocked traffic from your software or telepresence device going to 207.157.245.40
4. Keep a SIP session open for 5 or more minutes. This should catch any timer timeout issues.

### **For Assistance:**

Contact Josh Kaye-Carr at Channel Islands National Park at 805-658-5700 x5919 or x5810.

**\* Disclaimer of Endorsement:** Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by Channel Islands Live or its partners or affiliates. There are other options available, and you are encouraged to utilize whatever products or services that best suit your specific needs. Any specific reference contained herein shall not be used for advertising or product endorsement purposes.